

§ 5. Технічні засоби профілактики

Криміналістична техніка має велике значення у запобіганні злочинам. Одним із завдань сучасної криміналістичної науки є розроблення спеціальних захисних науково-технічних засобів та методів запобігання злочинності.

Технічні засоби профілактики розробляються на підставі вивчення та узагальнення слідчої, оперативно-розшукової та експертної практики, новітніх розробок у галузі захисту матеріальних цінностей та інформаційних ресурсів, виявлення причин та умов, що сприяли вчиненню злочинів. Важливим є вивчення типових способів вчинення певних видів злочинів з метою розробки науково-технічних засобів протидії злочинності.

Відмінність технічних засобів профілактики від інших криміналістичних засобів полягає в тому, що вони застосовуються до виникнення злочинного діяння. Використання таких засобів і методів має превентивний характер, перешкоджає вчиненню злочину або допомагає його виявленню.

Розвиток технічних засобів запобігання злочинам відбувається в таких головних напрямках:

- 1) удосконалення захисту документів від підроблення (розроблення бланків документів різних типів; пропонування певних реквізитів документів; нанесення спеціальних захисних сіток та інших елементів захисту; застосування поліграфічних особливостей виготовлення документів; використання спеціальних захисних чорнил чи відбитків печаток тощо);

- 2) розробка профілактичних приладів і пристроїв (наприклад, пристроїв охоронної сигналізації; електронних контролерів; приладів спостереження в нічний час; систем відеоспостереження за важливими об'єктами; пристроїв різних конструкцій проти викрадення транспортних засобів; хімічних засобів захисту тощо).

Злочинець під час взаємодії з такими приладами та пристроями залишає на місці події додаткові сліди. До науково-технічних засобів запобігання злочинам належать також засоби фіксації правопорушника на місці вчинення злочину. Це насамперед різноманітні хімічні пастки — спеціальні хімічні сполуки, що використовуються в профілактичній і оперативно-розшуковій діяльності для штучного слідоутворення. Потрапляючи на об'єкт, деякі спецсполуки викликають появу яскраво забарвлених слідів, що погано змиваються, або спричиняють люмінесценцію в ультрафіолетових променях. Розрізняють хімічні пастки активні (поєднання спецсполуки із пристроями викидання) і пасивні (слідоутворення відбувається під час контактних взаємодій). В оперативно-розшуковій діяльності використовуються

хімічні пастки «Купіль», «Катапульта» та уніфікована багаторазова хімічна пастка «Керн».

Технічні засоби профілактики тісно пов'язані з організаційними заходами запобіжного характеру. Це стосується порядку реєстрації документів, процедури видачі дозволів, наявності спеціальних правил обліку певних видів документів (наприклад, нотаріальних), певного порядку продажу вогнепальної чи холодної мисливської зброї та її обліку тощо.

Ефективне запобігання окремим видам або групам злочинів можливе за умови комплексного використання технічних засобів профілактики. Наприклад, запобігання шпигунству (ст. 114 КК), незаконному збиранню з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231 КК) та низці інших злочинів вимагає впровадження засобів криміналістичної профілактики за трьома основними напрямками:

1. Фізичний контроль доступу до будівель і приміщень.
2. Ідентифікація користувача електронно-обчислювальної машини (комп'ютера), радіоелектронного засобу, електронної інформаційної системи, транспортної телекомунікаційної мережі.
3. Фіксація правопорушника на місці вчинення злочину.

Фізичний контроль доступу до будівель і приміщень. Для забезпечення цього профілактичного напрямку можуть бути корисними напрацювання провідних мультибіометричних компаній і започаткована у 70-х рр. XX ст. технологія розумного (інтелектуального) будинку (*Smart House*), однією із невід'ємних складових якої є система захисту від несанкціонованого проникнення, де в єдиний комплекс об'єднано відеокамери, фотоелементи, що реагують на рух, детектори об'єму, контактні сенсори на поверхнях тощо, за допомогою яких здійснюється автоматична ідентифікація з використанням чипів радіочастотної ідентифікації *RFID* (*Radio Frequency Identification*), аналізаторів голосу, відбитків пальців рук чи райдужної оболонки ока. Наприклад, створений ученими університету Флориди (США) в рамках проекту *Gator-Tech Smart House* визначає місцезнаходження та положення фізичних осіб, що в ньому перебувають, а його «розумні двері» з використанням технології радіочастотної ідентифікації розпізнають осіб, доступ яким дозволено, та відчиняють перед ними двері без використання ключа. Функцію фізичного контролю

доступу здатні підтримувати імплантовані в тіло людини чіпи радіочастотної ідентифікації *RFID* (*Radio Frequency Identification*), що зазвичай дають змогу здійснювати: зберігання історії хвороби для екстрених випадків; вхід у приміщення, облаштовані системами безпеки; управління комп'ютерами й іншими пристроями за допомогою мозкових імпульсів; блокування больових сигналів при хронічних захворюваннях; зберігання паролів для комп'ютерних систем; взаємодію з *GPS* для пошуку осіб, що зникли безвісти і стеження за злочинцями.

Фонову ідентифікацію відвідувачів певних об'єктів здатна здійснювати і застосована Національним поліцейським відомством Японії комп'ютерна 3D-технологія, що автоматично розпізнає особу у натовпі, будує її об'ємну модель на основі двовимірного знімка й порівнює отримані дані з архівом. Для її функціонування достатньо звичайних камер спостереження та наявності в базі даних якісних знімків. Ця 3D-система дає можливість впізнати особу навіть при зміні її зовнішності шляхом використання перуки чи окулярів.

Ідентифікація користувача електронно-обчислювальної машини (комп'ютера), радіоелектронного засобу, електронної інформаційної системи, транспортної телекомунікаційної мережі. Відповідно до постанови Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29 березня 2006 р. № 373 ідентифікація — процедура розпізнавання користувача в системі, як правило, за допомогою наперед визначеного імені (ідентифікатора) або іншої апіорної інформації про нього, яка сприймається системою. Для вирішення проблеми безпеки інформаційних систем у більшості випадків застосовуються технології, що в тому чи іншому вигляді застосовують певні паролі (набори символів, карти з персональними ідентифікаційними кодами (*PIN*-карти) тощо). Існують «універсальні» системи ідентифікації, в яких користувачі для доступу на різні вузли використовують різні паролі, «зібрані» в одному місці. Однак символні паролі легко забути, загубити, вкрасти або зламати, а управління ними вимагає значних витрат.

Підвищення рівня безпеки інформаційних систем потребує впровадження біометричних технологій, найбільш поширеною серед яких є ідентифікація користувача за відбитками пальців рук на основі

наукових положень дактилоскопії. Стрімкий розвиток біометричних технологій пов'язаний із розширенням їх використання в персональних електронних секретарях, персональних комп'ютерах, мобільних телефонах, смартфонах, електронних планшетах тощо. Так, компанія *Sagem* запропонувала мобільний телефон із функціями ідентифікації користувача за відбитками пальців, а компанія *ASUS* облаштовує ноутбуки пристроями для зчитування відбитків пальців. У цьому напрямі *Identix* у співпраці з *Motorola* розробила технологію розпізнавання відбитків пальців *Identicator*, що знайшла застосування в апаратах і програмних продуктах цілої низки виробників, у тому числі: *Unisys*, *Compaq*, *IBM*, *Dell Computer* і *NEC*. Компанія *Ethentica* за участю *Philips Electronics* пропонує сканери для зчитування відбитків пальців та відповідне програмне забезпечення. Розробку аналогічних продуктів здійснює *Digital Persona* за фінансової підтримки *Intel* та *Kensington Technology*, а також *Veridicom*, за підтримки *Lucent Technologies* та *AT&T*. *AuthenTec* за сприяння *Harris Semiconductor* створила окрему мікросхему з сенсором, який реалізує функції захисту за відбитками пальців, що має назву *FingerLoc*. Навіть *USB*-брелоки різних виробників оснащуються функцією біометричного доступу.

Компанія «Альтоніка» здійснює серійне виробництво біометричних імобілайзерів серії «*Woodoo*», головною особливістю яких є ідентифікація за відбитками пальців володільця автомобіля. Таке технічне рішення забезпечує високу криптостійкість протиугінної системи та зручність в експлуатації, оскільки для відключення блокування двигуна вже немає потреби використовувати будь-які електронні ключі чи брелоки. Володільцю необхідно лише прикласти палець до скануючого модуля для порівняння папілярного візерунка із записаними у систему біометричними еталонами. При розпізнанні володільця система дозволяє запуск двигуна. Для розпізнавання відбитків пальців у біометричних імобілайзерах «*Woodoo*» використовується ємнісний сканер малого розміру, виконаний за передовою КМОП-технологією. Його зчитуюча поверхня надійно захищена зносостійким герметичним покриттям. На відміну від оптичного, який ніби «фотографує» палець, в ємнісному сканері напівпровідниковий пристрій реагує на кількість валиків і борозенок папілярного узору пальця. Їх індивідуальне поєднання утворює свій унікальний

електричний сигнал, який порівнюється зі збереженим у пам'яті еталоном. Біометричний сканер додатково пов'язаний з електроomeханічним замком, оскільки окремо взятий протиугінний пристрій малоефективний, а декілька таких систем, об'єднаних в єдиний комплекс, значно підвищують захищеність автомобіля від незаконного заволодіння ним.

Відомі й інші біометричні технології. Так, *IrisScan* пропонує спеціальні сканери, які дають змогу ідентифікувати користувача за райдужною оболонкою ока, що при помітно вищій вартості забезпечує й значно вищий рівень захисту інформації. *VeriVoice* створено технологію для ідентифікації особи за мовою *VeriVoice Security Lock*, що дає можливість ідентифікувати користувача не лише під час прямого контакту, а й дистанційно, наприклад за телефонним дзвінком. Голосове розпізнавання підтримується операційною системою від *Apple*. *Viisaga* розробила технологію ідентифікації користувачів за рисами обличчя. *Bioscrypt* розробила веб-камеру *3D DeskCam*, яка для біометричного сканування використовує інфрачервоні сканери і здатна знімати тривимірне зображення обличчя користувача для комп'ютерної ідентифікації. Основними параметрами, що враховуються під час сканування, є висота лоба, форма очей і перенісся. Камера легко ідентифікує користувача, який поголив бороду або вуса, успішно пройшла тестування і змогла відрізнити обличчя близнюків. *Samsung Electronics* упровадила в універсальному смартфоні систему безпеки *Face Recognition Unlock*, яка «впізнає» обличчя власника і автоматично розблоковує пристрій.

До невичерпного переліку унікальних розробок учені Національного університету м. Чжунсін (о. Тайвань) пропонують як комп'ютерний пароль використовувати ритми серця людини, адже шуми, темп скорочення, особливості роботи клапанів і міокарда є унікальними ідентифікуючими ознаками конкретної особи. А інженери Інституту передових промислових технологій (Японія) пропонують включити до переліку засобів ідентифікації особи, що вже традиційно використовуються в автопромисловості (електронні ключі, системи ідентифікації за відбитками пальців рук, рисами обличчя і голосом), автомобільне крісло, оснащене системою розпізнавання унікальної будови сидниць людини. До складу системи входять 360 вбудованих у крісло водія датчиків, що оцінюють рівень тиску,

який на них чинить та чи інша ділянка сидниць і стегон, після чого формується тривимірне відображення, за яким автомобільна електроніка упізнає автовласника.

Фіксація правопорушника на місці вчинення злочину. Серед техніко-криміналістичних засобів, що використовуються для запобігання злочинам, найбільше зацікавлення викликають ті, що ускладнюють або виключають можливість вчинення злочинного посягання. Одним із основних напрямів розвитку технічних засобів профілактики є розроблення профілактичних приладів і пристроїв, зокрема, пристроїв охоронної сигналізації, електронних контролерів, фотоелементів, реле, інших компонентів охорони периметру, замикальних і протигінних пристроїв різних конструкцій, шифр-систем, приладів відеоспостереження, мобільних відеореєструючих пристроїв, хімічних засобів захисту тощо. Намагаючись дезактивувати такі засоби, злочинець під час взаємодії з ними залишає на місці події додаткові сліди, що збільшує потік доказової інформації.

До науково-технічних засобів запобігання злочинам належать також засоби фіксації правопорушника на місці вчинення злочину. Це насамперед охоронні системи відеоспостереження та різноманітні хімічні пастки (маркери), арсенал яких постійно удосконалюється й поповнюється. Є відомим позитивний досвід використання у Великобританії та Австралії як активний маркер навіть ДНК-спрею «*SelectaDNA*», молекули якого містять унікальний ідентифікаційний код.

Запитання для самоконтролю

1. Що таке криміналістична техніка?
2. Що являють собою науково-технічні засоби?
3. Які існують галузі криміналістичної техніки?
4. Що являють собою інформаційні технології?
5. Які їх види і призначення?
6. Чи існує специфіка використання науково-технічних засобів у кримінальному провадженні?
7. Які комплекти науково-технічних засобів використовуються в діяльності слідчого?
8. Які завдання вирішує пересувна криміналістична лабораторія?
9. Які існують технічні засоби профілактики?

*Рекомендовано вченою радою Національного юридичного університету
імені Ярослава Мудрого (протокол № 4 від 26.10.2018 р.)*

Рецензенти:

В. В. Тищенко — доктор юридичних наук, професор, завідувач кафедри криміналістики Національного університету «Одеська юридична академія», член-кореспондент Національної академії правових наук України, заслужений діяч науки і техніки України;
М. Є. Шумило — доктор юридичних наук, професор, професор кафедри правосуддя Київського національного університету імені Тараса Шевченка, член-кореспондент Національної академії правових наук України, заслужений діяч науки і техніки України

Колектив авторів:

В. Ю. Шепітько, д-р юрид. наук, проф. (кер. авт. кол.) — вступ; розділи 1, 2, 4; § 1, 4 розділу 5; § 2, 3, 5 розділу 5 (у співавт.); розділ 6; § 1–8 розділу 7; § 1–3, 7, 9 розділу 8; розділи 9, 10, 12; § 1, 3 розділу 13; § 2 розділу 13 (у співавт.); § 1–5, 7, 8 розділу 14; § 3 розділу 15; розділ 16 (у співавт.); § 4–6 розділу 17; § 1, 3, 5–9, 12 розділу 18; § 4, 10 розділу 18 (у співавт.); § 1 розділу 19 (у співавт.); § 2–5 розділу 19; § 3, 4 розділу 21, § 1–4 розділу 22;
В. А. Журавель, д-р юрид. наук, проф. — § 2 розділу 15;
В. О. Коновалова, д-р юрид. наук, проф. — розділ 3; § 4, 5 розділу 15; § 1–3 розділу 17; § 2 розділу 18; розділ 20; § 1, 2 розділу 21;
В. М. Шевчук, д-р юрид. наук, проф. — § 6 розділу 14;
М. В. Шепітько, д-р юрид. наук, доц. — § 1 розділу 15;
Г. К. Авдєєва, канд. юрид. наук, доц. — § 9, 10 розділу 7; § 11 розділу 8; розділ 11;
В. І. Алексійчук, канд. юрид. наук, доц. — § 3 розділу 16 (у співавт.); § 10 розділу 18 (у співавт.); § 1 розділу 19 (у співавт.);
В. В. Білоус, канд. юрид. наук, доц. — § 2, 3, 5 розділу 5 (у співавт.); § 4–6, 8, 10 розділу 8; § 2 розділу 13 (у співавт.); § 1, 2 розділу 16 (у співавт.);
О. Ю. Булукув, канд. юрид. наук, доц. — § 9 розділу 14;
Є. С. Демідова, канд. юрид. наук — § 11 розділу 18;
О. М. Домашенко, канд. юрид. наук — § 6 розділу 15;
Д. В. Затеняцький, канд. юрид. наук — § 10 розділу 14;
О. В. Фунікова, канд. юрид. наук, доц. — § 4 розділу 18 (у співавт.);
В. О. Яремчук, канд. юрид. наук — § 5 розділу 22

Криміналістика : підручник : у 2 т. Т. 1 / [В. Ю. Шепітько, В. А. Журавель, К82 В. О. Коновалова та ін.] ; за ред. В. Ю. Шепітька. – Харків : Право, 2019. – 456 с.

ISBN 978-966-937-505-6

ISBN 978-966-937-542-1 (т. 1)

У першому томі підручника викладено загальнотеоретичні проблеми криміналістики, висвітлено питання криміналістичної техніки та окремих її галузей, розкрито зміст криміналістичної тактики. Поданий матеріал адаптовано до нових навчальних програм юридичних закладів вищої освіти та сучасних вимог.

Розраховано на студентів юридичних спеціальностей закладів вищої освіти, а також може бути корисним аспірантам, викладачам, науковцям та співробітникам органів правопорядку, суддям, адвокатам та іншим юристам.

УДК 343.98(075.8)

ISBN 978-966-937-542-1 (т. 1)
ISBN 978-966-937-505-6

© Шепітько В. Ю., Журавель В. А.,
Коновалова В. О. та ін., 2019
© Видавництво «Право», 2019

ЗМІСТ

ВСТУП	3
--------------------	---

ТЕОРЕТИЧНІ ЗАСАДИ КРИМІНАЛІСТИКИ

Розділ 1. ПОНЯТТЯ ТА ЗНАЧЕННЯ КРИМІНАЛІСТИКИ	5
§ 1. Предмет, система та завдання криміналістики	5
§ 2. Природа криміналістики	9
§ 3. Місце криміналістики в системі правових наук	11
<i>Запитання для самоконтролю</i>	13
Розділ 2. МЕТОДИ КРИМІНАЛІСТИКИ	14
§ 1. Процес пізнання у криміналістиці	14
§ 2. Класифікація методів криміналістики та їх види	16
<i>Запитання для самоконтролю</i>	19
Розділ 3. КРИМІНАЛІСТИЧНА ІДЕНТИФІКАЦІЯ	20
§ 1. Поняття ідентифікації	20
§ 2. Об'єкти, типи і види ідентифікації	21
§ 3. Загальна методика ідентифікації	24
<i>Запитання для самоконтролю</i>	27
Розділ 4. ІСТОРІЯ КРИМІНАЛІСТИКИ	28
§ 1. Виникнення і розвиток криміналістики	28
§ 2. Сучасний стан криміналістики в Україні	31
§ 3. Становлення експертних та криміналістичних установ в Україні	34
<i>Запитання для самоконтролю</i>	36

КРИМІНАЛІСТИЧНА ТЕХНІКА

Розділ 5. ЗАГАЛЬНІ ПОЛОЖЕННЯ КРИМІНАЛІСТИЧНОЇ ТЕХНІКИ	37
§ 1. Поняття криміналістичної техніки та її галузі	37
§ 2. Поняття інформаційних технологій у криміналістиці, їх види та значення	41

§ 3. Правові засади використання криміналістичної техніки.....	47
§ 4. Техніко-криміналістична оснащеність органів досудового розслідування.....	53
§ 5. Технічні засоби профілактики.....	57
<i>Запитання для самоконтролю.....</i>	63
Розділ 6. СУДОВА ФОТОГРАФІЯ ТА ВІДЕОЗАПИС	64
§ 1. Поняття судової фотографії та її значення.....	64
§ 2. Види та методи судово-оперативної фотозйомки	66
§ 3. Судово-дослідницька фотографія	76
§ 4. Криміналістичний відеозапис.....	77
<i>Запитання для самоконтролю.....</i>	80
Розділ 7. ТРАСОЛОГІЯ	82
§ 1. Поняття трасології та її значення	82
§ 2. Поняття сліду в трасології. Механізм слідоутворення	83
§ 3. Класифікація слідів.....	85
§ 4. Основи дактилоскопії.....	87
§ 5. Виявлення, фіксація і вилучення слідів рук. Сутність дактилоскопічної експертизи	90
§ 6. Сліди ніг і взуття людини	94
§ 7. Сліди знарядь злочину та інструментів.....	97
§ 8. Сліди транспортних засобів.....	99
§ 9. Криміналістичне дослідження замикальних та запобіжних (контрольних) засобів	100
§ 10. Встановлення цілого за частинами	104
<i>Запитання для самоконтролю.....</i>	107
Розділ 8. КРИМІНАЛІСТИЧНЕ ДОСЛІДЖЕННЯ ЗБРОЇ.....	108
§ 1. Поняття судової балістики та її значення.....	108
§ 2. Криміналістична класифікація вогнепальної зброї та види боєприпасів.....	109
§ 3. Сліди дії вогнепальної зброї, їх види.....	115
§ 4. Поняття криміналістичної вибухотехніки та її значення.....	117
§ 5. Криміналістична класифікація вибухових речовин і вибухових пристроїв	121
§ 6. Сліди, пов'язані з використанням вибухових матеріалів	127
§ 7. Слідчий огляд вогнепальної зброї та слідів її дії.....	129
§ 8. Слідчий огляд у кримінальних провадженнях щодо подій, пов'язаних із використанням вибухових матеріалів.....	131